REMARKS/ARGUMENTS

Rejections under 35 U.S.C. § 102

§ 102 Rejections based on Yeung et al.

Claims 1-14, 17-29, 31-35, 37, 38, 47-56, 59, 66-68 stand rejected as allegedly anticipated by U.S. Patent No. 6,668,246 issued to Yeung et al. (hereafter "Yeung et al."). See Page 2 of the April 12, 2005 Office Action.

Claim 1 (and all claims depending therefrom) and Claim 66 (and all claims depending therefrom)

In order for a reference to anticipate a claim, the reference must disclose each and every limitation of the claimed invention, either expressly or inherently, such that a person of ordinary skill in the art could practice the invention without undue experimentation. See Atlas Powder Co. v. Ireco Inc., 190 F.3d 1342, 1347, 51 USPQ2d 1943, 1947 (Fed. Cir. 1999); In re Paulsen, 30 F.3d 1475, 1479, 31 USPQ2d 1671, 1673 (Fed. Cir. 1994). Newly Amended Independent Claim 1 recites, inter alia, "A method for securing a data object, comprising: providing an openly accessible data object comprising digital data and file format information; embedding independent data into the openly accessible data object; and scrambling the openly accessible data object to degrade the openly accessible data object to a predetermined signal quality level where at least a portion of the independent data can be decoded from the scrambled openly accessible data object." The 102 rejection based on Yeung et al. is improper for at least the reason that Yeung et al. fails to disclose [emphasis added] (1) "providing an **openly accessible data object** comprising digital data and file format information" (2) "scrambling the openly accessible data object to degrade the openly accessible data object to a predetermined signal quality level **where at least a portion of the independent data can be decoded from the scrambled openly accessible data object**" as required by the rejected claims. The encrypted data of Yeung et al. is *de facto* inaccessible. This teaches away from the Applicants "openly accessible data objects" for evaluation and subsequent purchase, in a plurality of signal quality levels. The 102 rejection is similarly flawed for Newly Amended Independent Claim 66 (and all dependent claims), as Yeung et al. does not disclose (1) an "embedder" (2) a "scrambler" and (3) "a decoder that can decode at least a portion of the independent data from the scrambled openly accessible data object" as required by the claim limitations. Yeung et al. apparently describes a conditional access scheme for which "content requests" by users must always be authenticated *prior* to playback or other use of said content-- data objects are not "openly accessible", nor is independent data decodable from the alleged scrambled object of Yeung et al. [emphasis added]:

> A content distribution system comprising a server platform and a client platform. The server platform **includes a memory unit to store digital content and *access control logic to activate content protection mechanisms that provide multiple levels of access protection* to the digital content,** Yeung et al at Abstract.

Figures 2, Figure 4, and Figure 9 provide depictions of content passing to users *for authentication then authorization in an encrypted state*. "Content" is labeled as "290" in the figures and description. No "openly accessible data object" is described, teaching away from the present invention [emphasis added]:

> After **one or both** of the scrambling schemes has been performed, **the resultant content 290 (*encrypted and/or* visually or perceptually distorted) is delivered over a secure communication link such that no eavesdroppers can *reliably recover the original video in its digital form***. Yeung et al at Col. 6 ll. 47-51.

To deliver such secured data teaches that the system of Yeung et al. cannot recover "at least a portion of the independent data from the scrambled openly accessible data object", required by the claim[s]. In fact, by "controlling access" with a "successful replication of key(s)"— a component of blanket access restriction, Yeung et al. cannot anticipate "decoding" "independent data from the scrambled openly accessible data object"-- a significant advantage over Yeung et al. taught by the present invention. One *must know* pre-authorized information, to "replicate" the keys, to access *any* of Yeung et al.'s content:

> Referring to FIG. 4, an illustrative block diagram of an embodiment of a client platform 120 is shown. Upon delivery, content 290 is stored in a memory unit 410. After being delivered in its entirety or in part during content streaming, client platform 120 fetches its client identifier and/or other auxiliary information and attempts to replicate key(s) produced at server platform 110. ***The degree of successful replication of key(s) controls the level of access to delivered content 290***. Yeung at Col. 7 ll. 44-54.

Yeung et al.'s conditional access system cannot support "openly accessible data objects" nor the benefits of "try-before-you-buy" functionality, including: multiple levels of predetermined quality, measurements of bandwidth use, and payment schemes dependent on relationships between "embedded independent data" and the "scrambled openly accessible data objects". In the case where processing happens on a "client platform" (e.g., Figure 9), content is encrypted at the client side, again teaching away from the present invention, and any optional and alleged "watermark insertion keys" taught by Yeung et al. are "discarded after use" limiting any functional means for measuring signal quality, bandwidth, or payment "openly accessible data object" use when "at least a portion of the independent data can be decoded from the scrambled openly accessible data object" – required by the claim limitation[s].

Conditional access schemes have the inherent property of requiring authorization or authentication *prior* to any decryption or "data descrambling":

> The present invention relates to a platform and corresponding method to protect content from unauthorized observation and/or manipulation

> through hardware-based identification and a variety of content protection mechanisms. **Selected combinations of content protection mechanisms combined with hardware-based identification can provide different levels of access control. Each level of access control is associated with a unique degree of protection against unauthorized observation and/or manipulation of content**. Yeung et al. at Col. 2 ll. 28-38.

Yeung et al. even restricts storage and "other use" when the "client platform" is used for substantially all of the conditional access logic (Yeung et al. at Col. 9 ll. 45-50): "The visual/perceptual scrambling process 270 is also identical to the above-identified scheme described in FIG. 2. Content 900 and watermark insertion key 920 can optionally be encrypted prior to transmission, **in which case client platform 120 is responsible for decrypting and subsequently *re-encrypting content 900 prior to storage or other use***." By failing to provide "openly accessible data objects" even on a "client platform", as per Figure 9, clearly, Yeung et al. cannot meet the limitations of the instant invention's claims and teaches away from the significant benefits of the present invention.

Because Yeung et al. fails to disclose (1) "providing an openly accessible data object comprising digital data and file format information" (2) "scrambling the openly accessible data object to degrade the openly accessible data object to a predetermined signal quality level where at least a portion of the independent data can be decoded from the scrambled openly accessible data object" as required by Claim 1, the Section 102 rejection of Claim 1 must be withdrawn. Similarly, Yeung et al. fails to disclose (1) an "embedder", (2) a "scrambler", and (3) "a decoder that can decode at least a portion of the independent data from the scrambled openly accessible data object" as required by Claim 66. Moreover, for the same reasons that Claim 1 and Claim 66 are patentable over Yeung et al., the claims that depend from Claim 1 and Claim 66 are also patentable. Applicants request the Examiner withdraw the Section 102 rejections of Claims 1 and 66 and all claims depending therefrom based on Yeung et al.

Claims 21, 31 and 49

Applicants respectfully disagree with the Examiner's assertion that Yeung et al. meet the claim limitations of Newly Amended Independent Claims 21, 31 and 49. Yeung et al., as argued previously, teaches an alleged conditional access scheme from which "at least a portion of" embedded "independent authentication data" (Claim 21 and all claims depending therefrom) or "independent data" (Claim 31 and 49 and all claims depending therefrom) ***cannot*** be decoded from a "manipulated data object" (Claim 21 and all dependent claims); "scrambled data object" (Claim 31 and all dependent claims); or, "scrambled data signal" (Claim 49 and all dependent claims). In each case, Yeung et al. requires her alleged "scrambled data object" to first be decrypted, then descrambled *prior to optional* and alleged "watermark extraction". In fact, the data of Yeung et al. is stored in such a manner that "open access", as taught by the Applicants, is considered "sabotage", teaching away from the claimed invention[s] of the Applicants'.

> The descrambled and decrypted data blocks are temporarily stored in a memory unit after decryption and/or descrambling operations are performed for displaying content in the data blocks. **However, a substantial portion or the entire content need not be decrypted or descrambled and stored on permanent storage for the content to be played. This increases the difficulty to sabotage content.** Yeung et al. Col. 8 ll. 22-28.

Further, additional claim limitations for Claim 21, 31 and 49 (and all claims depending therefrom), indicate significant benefits over Yeung et al. Yeung et al. teaches away from these additional required claim elements, including: "distributing the manipulated data object where access to the manipulated data object in not conditional" (Claim 21); and, (1) "distributing at least one predetermined key that enables access to the data object, the embedded independent data, or both the data object and the embedded independent data"; (2) "decoding at least a portion of the independent data from the scrambled data object with the predetermined key"; and (3) "descrambling the scrambled data object with the predetermined key" (claim 31). Figure 4 specifically indicates that ***strictly*** encrypted content ("290") must first undergo "data descrambling 420" ***and*** "visual/perceptual descrambling 430" prior to "watermark extraction 440"—teaching away from the significant benefits of the instant invention[s]. As described, no data passes through Yeung et al. without at least being encrypted. It is respectfully submitted that the Examiner has failed to establish a case of anticipation. Applicants therefore request the Examiner to withdraw the Section 102 rejections for Claims 21, 31 and 49 (and all claims depending therefrom) based on Yeung et al.

Claims 14 and 68

Applicants respectfully disagree with the Examiner's assertion that Yeung et al. meet the claim limitations of Newly Amended Independent Claims 14 and 68 (and all claims depending therefrom). Yeung et al., as argued previously, teaches an alleged conditional access scheme for which her alleged "scrambled" data, if optionally applied, is always and inherently encrypted, as argued previously. Yeung et al. argue that scrambling is performed to distort in such a manner as to leave the content "substantially inferior to the original form" (Col. 11. 3-5) but within the context of having to be encrypted as well, leaving no presumption of *multiple* levels of scrambling, e.g. at least 2 levels of scrambling, or signal degradation, as required by the claims. This teaches away from the claim limitations of Claim 14 and 68. Simply, by primarily relying on encryption ***and*** conditional access, no additional levels of signal degradation are anticipated or disclosed by Yeung et al. As argued previously, there is no teaching of decoding independent data embedded within the **scrambled** content. Nor does Yeung et al. teach creating at least two keys for descrambling, let alone levels of degradation which can be differentiated by the created "descrambling key[s]". Further, Yeung et al. does not disclose scrambling "where at least a portion of embedded data can be decoded from the scrambled digital signal". It is respectfully submitted that the Examiner has failed to establish a case of anticipation. Applicants therefore request the Examiner to withdraw the Section 102 rejections for Claims 14 and 68 (and all claims depending therefrom) based on Yeung et al.

Claim 60, 63 and 64

Applicants respectfully disagree with the Examiner's assertion that "... Miller et al. teaches a method for bandwidth allocation...", April 12, 2005 Office Action at Page 11. The 102 rejection is improper for at least the reason that Miller et al. fails to disclose (1) "presenting a plurality of openly accessible data objects to a user, each data object having a security application, where the security applications comprises embedding, scrambling, or both embedding and scrambling"; (2) "linking at least a first data object to at least one second data object"; or (3) "wherein a characteristic of the first data object causes a change in the second data object". Miller et al. allegedly teaches a means for implementing messaging between independent object-oriented applications— clearly teaching away from "presenting a plurality of openly accessible data objects to a user, each data object having a security application, where the security applications comprises embedding, scrambling, or both embedding and scrambling". These objects are "executables" not data objects for which quantity or quality can be linked, "embedding" can be performed, and impacted by changes to one or the other linked object, as required by the claim limitation[s]. "Bandwidth allocation" is not disclosed or mentioned by Miller et al.: the alleged "objects" of Miller et al. are not linked—they are not "openly accessible", a required claim element. Miller et al. apparently discloses access restrictions to his "executable" objects. Not only by requiring encryption, for "right of access" to his alleged object (Miller et al. at Col. 10 ll. 5-10) but even proxy's by which *the system*, independent of the objects themselves, must communicate *between* objects. This clearly means that objects *cannot be linked* in such a manner that "a characteristic of the first data object causes a change in the second data object"—required by the claims. Miller et al. states that "[e]ach process provides a registrar that includes a secret code table wherein an object is registered with a unique, practically unguessable secret code" (Miller et al. at Abstract). Miller et al. does not teach "security applications comprises embedding, scrambling, or both embedding and scrambling" required by Independent Claim 60, from which Claim 63 and 64 depend.

Significantly, a "transport manager" is *required* by Miller et al. (Col. 10 ll. 57 – Col. 11 ll. 17)—teaching away from linking of "openly accessible data objects" and the claimed invention[s]. This is a clear departure from the Applicants' claimed invention[s] for enabling open access to a plurality of data objects where said objects may be linked and bandwidth may be effectively allocated based on said linking. Miller et al. clearly requires that each object be independent from the transport managers: "... because all security and inter-process message transmission functions are handled by the transport manager... ", in fact "... [a]ll local messages are passed using language-level pointers with security provided by the operating system or the computer language" (Miller et al. at Col. 11 ll. 8-17). This apparently relates to basic encrypted objects for which linking, as argued by the Applicants, is not possible. Embedding is simply not disclosed or even possible with alleged encrypted objects of Miller et al. The present invention provides significant advantages over Miller et al. by requiring these claim limitations: (1) "where the security applications comprises embedding, scrambling, or both embedding and scrambling;" (2) "linking at least a first data object to at least one second data object" (3) "wherein a characteristic of the first data object causes a change in the second data object". For these reasons the Applicants

respectfully request the Examiner to withdraw the Section 102 rejections for Claim 60 and all claims depending therefrom based on Miller et al.

Rejections under 35 U.S.C. § 103

In order to "establish a prima facie case of obviousness, three basic criteria must be met." MPEP § 7.06.02(j). First, there must be some motivation or suggestion to modify the reference or to make the proposed combination. Second, there must be a reasonable expectation of success. "The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on the applicant's disclosure." MPEP § 2142 (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)). Third, the combined references must teach or suggest all claim limitations.

The Examiner has failed to establish a *prima facie* case of obviousness to the extent that there is no motivation or suggestion to make the proposed combinations of the references as directed by the Examiner. According to the MPEP,

> [i]n order to support a conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner *must present a convincing line of reasoning* as to why the artisan would have found the claimed invention obvious in light of the teachings of the references.

MPEP 2142 (citing *Ex parte Clapp*, 277 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985)) [emphasis added]. Further, "[w]hen the motivation to combine the teachings of the references is not immediately apparent, it is the duty of the examiner to explain why the combination of teachings is proper." MPEP 2142 (citing *Ex Parte Skinner*, 2 USPQ2d 1788 (Bd. Pat. App. & Inter. 1998)).

The Federal Circuit has recently emphasized the importance of providing evidence of motivation to combine in *Winner Int'l Royalty Corp. v. Ching-Rong Wang*, 202 F. 3d 1340, 1348-49 (Fed. Cir. Jan. 27, 2000). "Although a reference need not expressly teach that the disclosure contained therein should be combined with another . . . the showing of combinability, in whatever form, must nevertheless be 'clear and particular.'" *Winner*, 202 F. 3d at 1348-49 (citations omitted). Further, the "absence of such a suggestion to combine is *dispositive* in an obviousness determination." *Gambro Lundia AB v. Baxter Healthcare Corp.*, 11 F.3d 1573, 1579 (Fed. Cir. 1997) [emphasis added].

Applicants submit that the Examiner has not satisfied his initial burden of providing "clear and particular" evidence of motivation to combine for any of the proposed combinations of references. More significantly, the references, even in combination, do not disclose all elements of the Applicants' claimed invention[s].

§ 103 Rejections based on Yeung et al. in view of Hirose.

Claims 15, 16, 32, 57 and 58 have been rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Yeung et al (U.S. Patent No. 6,668,246) in view of Hirose (U.S.

Patent No. 5,917,915). Examiner asserts that " ... Hirose teaches associating a first, second, and third payment level with the associated data signals ...", April 12, 2005 Office Action at Page 12. This assertion is unsupported. Yeung et al. does not teach a "first scrambling technique where at least a portion of embedded data can be decoded from the scrambled digital signal" let alone from a second scrambled state, as required in Independent Claim 14, from which claims 15 and 16 depend. Hirose teaches encryption of data. In fact, Hirose requires that users first pay or subscribe to data *prior to receiving it* (Hirose at Col. 2 ll. 5-15). Yeung et al. apparently teaches a similar scheme-- as argued previously. Neither reference discloses accessible data objects for evaluation or purchase, based on a payment level.

Second, the combination fails to disclose all of the elements of Independent Claims 14, 31 and 49 and all claims that depend therefrom, including Claims 15, 16, 32, 57 and 58. That neither reference mentions "first scrambling technique where at least a portion of embedded data can be decoded from the scrambled digital signal" (Claim 14); "scrambling the data object where at least a portion of the independent data can be decoded from the scrambled data object" (Claim 31); and, "applying a scrambling technique selected from the group consisting of file format manipulation and partial encryption where at least a portion of the embedded independent data can be decoded from the scrambled data signal" (Claim 49) indicates a lack of all claim elements of the present invention. The combination of the two does not disclose all of the elements of the claimed invention[s]; therefore, the Section 103 rejection is improper. By offering accessible data objects that are scrambled at predetermined signal quality levels, unlike the teachings of Yeung et al. and Hirose which *restrict access*, choices over a payment level can be made.

Third, there is no motivation to combine Yeung et al. with Hirose. Neither discloses any form of scrambling from which embedded data can be detected or decoded, as per the Applicants' invention, and each appears to apply encryption in a manner as to require prior authorization to gain access to data. No data is presented with open access. With the instant invention, as the signal quality improves, more embedded independent data is recovered, and payment levels can be adjusted—there is no teaching of this in either Yeung et al. or Hirose. Where is the motivation to combine? Each reference, even in combination, teaches away from embedding independent information and subsequently scrambling to predetermined signal quality levels where the embedded information may be recovered from the scrambled information—preventing payment analysis in a manner described by the claimed invention[s]. For at least these reasons Applicants respectfully request the Section 103 rejections to be withdrawn.

§ 103 Rejections based on Yeung et al. in view of Binding et al.

Claims 30, 36, 39-42, and 46 has been rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Yeung et al. (U.S. Patent No. 6,668,246) in view of Binding et al. (U.S. Patent No. 6,775,772). Examiner asserts that " ... Binding et al. teaches generating an authorization key that is dependent on a public and a private key, wherein the authorization key is further dependent on at least one of a time, a channel, and an object," April 12, 2005 Office Action at Page 14. This assertion is unsupported. For at least

the reasons discussed above, and further argued here, neither Yeung et al., nor Binding et al., even in combination discloses "embedding" and "scrambling" where the embedded data may be detected or decoded from the scrambled data as required by the Applicants' claim limitations. Binding et al. allegedly teaches a means for "piggy-backed key exchange" *but* an "authorization key" is *not* disclosed. Binding et al. apparently discloses "a value created by a random number generator" (Col. 9 ll. 64) from which a sender and receiver digitally sign the "nonce" (Col. 10 ll. 1-15). It is unclear how this relates to "authorization keys" as taught by the instant invention[s]. In fact, the session data is encrypted which would prevent any ability to descramble the data and recover embedded data from the openly accessible and scrambled data objects of the claimed invention[s].

Second, the combination fails to disclose all of the elements of Independent Claims 21 and 31 and all claims that depend therefrom, including Claims 30, 36, 39-42, and 46. That neither reference mentions "manipulating the file format information based on at least one signal characteristic of the data object" (Claim 21) or "scrambling the data object where at least a portion of the independent data can be decoded from the scrambled data object" (Claim 31) indicates that the combination cannot offer the significant advantages of the claimed invention[s]. Furthermore, additional claim elements cannot be remedied by either reference, even in combination. The claims require that "at least a portion of" embedded "independent authentication data" (Claim 21 and all claims depending therefrom) or "independent data" (Claim 31 and all claims depending therefrom) ***can*** be decoded from a "manipulated data object" (Claim 21 and all dependent claims) or "scrambled data object" (Claim 31 and all dependent claims). The combination of the two does not disclose all of the elements of the claimed invention[s]; therefore, the Section 103 rejection is improper. By offering accessible data objects that are scrambled at predetermined signal quality levels, unlike the teachings of Yeung et al. and Binding et al. which *restrict access*, choices over how "authorization keys", "time stamps", or "session keys" may be used to affect data quality or quantity can be made.

Third, there is no motivation to combine Yeung et al. with Binding et al. Neither discloses any form of scrambling from which embedded data can be detected or decoded, as per the Applicants' invention, and each appears to apply encryption in a manner as to require prior authorization to gain access to data—though neither distributes a key to access the data object *and/or* the embedded data. Yeung et al. is directed at access controlled "content" and Binding et al. is directed at "piggy-backed keys" which rely on encrypted key exchange. No data is presented with open access. Where is the motivation to combine? Each reference, even in combination, teaches away from embedding independent information and subsequently scrambling to predetermined signal quality levels where the embedded information may be recovered from the scrambled information, where " the authorization key is further dependent on at least one of a time, a channel, and an object", let alone utilizing "time stamps" or "session keys" in the descrambling process. For at least these reasons Applicants respectfully request the Section 103 rejections to be withdrawn.

§ 103 Rejections based on a combination of Yeung et al. in view of Pietropaolo et al.

Claims 43-45 have been rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Yeung et al. (U.S. Patent No. 6,668,246) in view of Pietropaolo et al. (U.S. Patent No. 6,351,765). Examiner asserts that "Pietropaolo et al. teaches the step of descrambling the scrambled data object comprises logically associating a signal quality level with a predetermined estimation of a bandwidth requirement for a session," April 12, 2005 Office Action at Page 16. Applicants respectfully disagree. First, Yeung et al. never mentions bandwidth allocation, let alone, allocation based on scrambling or descrambling of data objects. Significantly, Independent Claim 31, from which Claims 43-45 depend, requires "scrambling the data object where at least a portion of the independent data can be decoded from the scrambled data object". Additional arguments were previously presented above in connection with the Section 102 rejections.

Second, where is the motivation to combine Yeung et al. with Pietropaolo et al.? Pietropaolo et al. does not disclose any "scrambling" or "descrambling" from which the present invention subsequently determines "bandwidth requirements". Pietropaolo et al. apparently describes a "nonlinear video editing system" from which the access restrictions of Yeung et al. would act as an impediment to any editing or manipulation of "nonlinear video". The arguments associated with Yeung et al. were made in connection with the Section 102 rejections above.

> The present invention relates to a platform and corresponding method to protect content from unauthorized observation and/or manipulation through hardware-based identification and a variety of content protection mechanisms. **Selected combinations of content protection mechanisms combined with hardware-based identification can provide different levels of access control. Each level of access control is associated with a unique degree of protection against unauthorized observation and/or manipulation of content.** Yeung et al. at Col. 2 ll. 28-38.

Third, there is no motivation to combine Yeung et al. with Pietropaolo et al. Neither discloses any form of scrambling from which embedded data can be detected or decoded, as per the Applicants' claim limitations, preventing measurements of bandwidth or signal quality associated with descrambling required by the dependent claim limitations. Yeung et al. would prevent any distribution for content editing since access is inherently restricted. Where is the motivation to combine? Each reference, even in combination, teaches away from embedding independent information and subsequently scrambling to predetermined signal quality levels where the embedded information may be recovered from the scrambled information, for "logically associating a signal quality with a predetermined estimation of a bandwidth requirement for the session", "logically associating a signal quality with a bandwidth allocation model", "logically associating a signal quality with a signal quality parameter" – all required claim elements. For at least these reasons Applicants respectfully request the Section 103 rejections based on Yeung et al. in view of Pietropaolo et al. be withdrawn.

§ 103 Rejections based on a combination of Miller et al. in view of Allen

Claim 61 has been rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Miller et al. (U.S. Patent No. 6,049,838) in view of Allen (U.S. Patent No. 5,418,713). Examiner asserts that "Allen teaches wherein the first data object comprises advertising"," April 12, 2005 Office Action at Page 17. Miller et al. apparently discloses access restrictions to his "executable" objects—they could not be "advertising" as required in the claim. Not only by requiring encryption, for "right of access" to his alleged object (Miller et al. at Col. 10 ll. 5-10) but even *proxy*'s by which the system must communicate between objects. This clearly means that objects *cannot be linked* in such a manner that "a characteristic of the first data object causes a change in the second data object"—required by the claims. Miller et al. states that "[e]ach process provides a registrar that includes a secret code table wherein an object is registered with a unique, practically unguessable secret code" (Miller et al. at Abstract). A "transport manager" is *required* by Miller et al. (Col. 10 ll. 57 – Col. 11 ll. 17). Allen discloses "duplicat[ion] of original content recordings" (Allen at Abstract) a plurality of data objects would presumably mean duplicates of an original. No linking of "openly accessible data objects" is disclosed by Allen nor Miller et al. Further, Allen's does not disclose a "security application" and, any alleged advertising is associated with a *predetermined* customer identification (Col. 14 ll. 30-45). A user is not provided with "a plurality of openly accessible data objects", but titles alone, Allen at Col 12 ll. 47 – Col. 13 ll. 2, again, teaching away from the claim elements of the present invention.

Second, where is the motivation to combine Miller et al. and Allen? Miller et al.'s object oriented executables have inherent access restrictions and are not data objects for which "a characteristic of the first data object causes a change in the second data object". Allen discloses duplication of "original content recording" for which it would likely follow that any other object would be duplicated separately from the first data object. Duplication is not linking-- each alleged object of Allen is simply copied as is. Miller et al. teaches a similar approach in maintaining a "transport manager" between executable objects, no linking for either reference could be anticipated. Neither teaches "security applications comprises embedding, scrambling, or both embedding and scrambling", required by Independent Claim 60, from which Claim 61 depends.

Third, there is no motivation to combine Miller et al. and Allen. Miller et al. discloses a means for access restricted object-oriented "executables": Allen discloses duplication and thus unfettered copying of content. Neither addresses relationships between linked objects for which a changes in one object causes changes in the linked second object. Applicants respectfully request the Section 103 rejections based on Miller et al. in view of Allen be withdrawn.

§ 103 Rejections based on a combination of Miller et al. in view of Hirose et al.

Claim 62 and 65 has been rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Miller et al. (U.S. Patent No. 6,049,838) in view of Hirose et al. (U.S. Patent No. 5,917,915). Examiner asserts that "Hirose et al. teaches an increased quantity of the first data object causes a signal quality level of the second data object to increase," April 12, 2005 Office Action at Page 18. Miller et al. apparently discloses access restrictions to his "executable" objects. Not only by requiring encryption, for "right of access" to his alleged object (Miller et al. at Col. 10 ll. 5-10) but even *proxy*'s by which the system must

communicate between objects. This clearly means that objects *cannot be linked* in such a manner that "a characteristic of the first data object causes a change in the second data object"—required by the claims. Miller et al. states that "[e]ach process provides a registrar that includes a secret code table wherein an object is registered with a unique, practically unguessable secret code" (Miller et al. at Abstract). A "transport manager" is *required* by Miller et al. (Col. 10 ll. 57 – Col. 11 ll. 17). Hirose allegedly teaches a means for encrypting "newspaper data" for broadcast. The approach encrypts the data, making it unobservable, and encrypts the "transfer channel", independent of the data. Hirose never mentions any linking of data objects for "signal quality level" increase (Claim 62) or payment adjustment (Claim 65), nor a means for one data object to cause a change in a separate data object. In fact, Hirose teaches away from the Applicants' claimed invention[s] by requiring that at least one "newspaper data" be encrypted separately from other "newspaper data". Hirose is also directed at "authorized subscribers" (Col. 3 ll. 2-15), not producing "openly accessible data objects" linked to changes in "quality" and "quantity" of the data object[s] signal, as required by the claim elements.

Second, where is the motivation to combine Miller et al. with Hirose et al.? Neither teaches "security applications comprises embedding, scrambling, or both embedding and scrambling", required by Independent Claim 60, from which Claim 62 and 65 depends. Hirose specifically discloses that each type of date is encrypted using separate keys, clearly teaching away from the instant invention. "Each type of news data is encoded according to a unique predetermined encryption [sic] key (first key data) associated with each type of news data. That is, each type of news data is encoded/encrypted with different first key data", Hirose at Col. 2 ll. 60-65). Miller et al. and Hirose do not anticipate the claim elements of the instant invention, singularly or in combination. Neither addresses "openly accessible data objects", both, instead, focused on encrypted, inherently inaccessible data.

Third, there is no motivation to combine Miller et al. with Hirose et al. Signal quality plays no role in the schemes of Miller et al. and Hirose et al. as independent objects are served up as individually encrypted objects for which linking is not possible with other data objects. Applicants respectfully request the Section 103 rejections based on Miller et al. in view of Hirose be withdrawn.

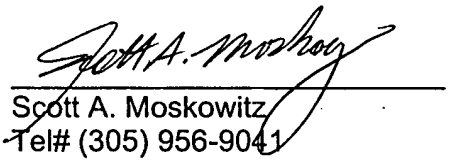
Conclusion

Applicants maintain that this application is in condition for allowance, and such disposition is earnestly solicited. If the Examiner believes that an interview with the Applicants, either by telephone or in person, would further prosecution of this application, we would welcome the opportunity for such an interview.

It is believed that no other fees are required to ensure entry and consideration of this response.

Respectfully submitted,

Date: July 12, 2005

By: 

Scott A. Moskowitz
Tel# (305) 956-9041